NAJWYŻSZA IZBA KONTROLI

Delegatura w Katowicach

LKA.410.12.4.2025

Pan
Maciej Mrówka
Wójt Gminy Wilkowice
Urząd Gminy w Wilkowicach
ul. Wyzwolenia 25
43-360 Wilkowice

WYSTĄPIENIE POKONTROLNE

P/25/003/LKA - Realizacja projektu Cyberbezpieczny Samorząd

NAJWYŻSZA IZBA KONTROLI
Delegatura w Katowicach
ul. Powstańców 29, 40-039 Katowice
tel. 48327844200, lka@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Gminy w Wilkowicach, ul. Wyzwolenia 25, 43-360 Wilkowice[1]
Kierownik jednostki kontrolowanej	Maciej Mrówka, Wójt Gminy Wilkowice[2], 14 maja 2024 r. do nadal W okresie objętym kontrolą funkcję kierownika jednostki poprzednio pełnili: Janusz Zemanek, Wójt Gminy Wilkowice, 20 listopada 2018 r. do 14 maja 2024 r.
Zakres przedmiotowy kontroli	Realizacja przez gminy i powiaty działań w celu zwiększenia poziomu cyberbezpieczeństwa.
Okres objęty kontrolą	Od 1 stycznia 2023 r. do dnia zakończenia czynności kontrolnych, tj. do 20 sierpnia 2025 r.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[3]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Katowicach
Kontroler	Magdalena Śleziak, specjalista kontroli państwowej, upoważnienie do kontroli nr LKA/124/2025 z 24 czerwca 2025 r.

(akta kontroli str. 1-2)

[1] Dalej: Urząd lub Gmina.
[2] Dalej: Wójt.
[3] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK.

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

W Urzędzie rozpoznawano potrzeby w zakresie zwiększenia poziomu cyberbezpieczeństwa, które ujęto w: *Strategii Rozwoju Gminy Wilkowice do roku 2030,* audycie wewnętrznym *Bezpieczeństwo informacji w 2023 r.*[5], oraz w analizie ryzka przeprowadzonej w 2023 r. na poziomie zidentyfikowanych ryzyk w obszarze przetwarzania i ochrony danych osobowych. Gmina we wniosku o przyznanie grantu[6] nie określiła wskaźników produktu i rezultatu, wniosek ten został zaakceptowany przez Centrum Projektów Polska Cyfrowa[7]. W trakcie kontroli Urząd wskazał jakie wskaźniki rezultatu planuje rozliczyć. Gmina przekazała *Ankietę Dojrzałości Cyberbezpieczeństwa* do Operatora[8] z zachowaniem terminu i formy określonej w umowie o powierzenie grantu[9], zawartej 26 lipca 2024 r. z CPPC, w ramach której przyznano dofinansowanie na realizację projektu pn. *Cyberbezpieczny Urząd Gminy w Wilkowicach*[10], w kwocie 848 240,02 zł[11]. Łączna kwota wydatków na realizację Projektu wyniosła 1 131 999,75 zł[12] (z czego dofinansowanie ze: środków budżetu państwa 135 471,84 zł, środków UE 711 227,16 zł i środków własnych 285 300,75 zł). Grant wykorzystano w wysokości 846 699 zł. Poniesione wydatki zostały zrealizowane zgodnie z wytycznymi dotyczącymi kwalifikowalności wydatków oraz w ramach limitów zatwierdzonych we wniosku o przyznanie grantu.

Stwierdzone nieprawidłowości dotyczyły:

- nieustanowienia i niewdrożenia kompletnego Systemu Zarządzania Bezpieczeństwem Informacji, o którym mowa w §19 ust. 1 w związku z ust. 3 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[13];
- niewypełnienia obowiązku określonego w § 19 ust. 2 pkt 14 rozporządzenia KRI tj. zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok; czyli w Urzędzie audyt powinien być przeprowadzony najpóźniej w grudniu 2024 r.,
- braku analizy ryzyka w 2024 r. wymaganej zarządzeniem wewnętrznym Urzędu;
- niestosowania procedury przyznawania uprawnień w systemach informatycznych w zakresie ich przydziału do korzystania z zasobów sprzętowych, co było niezgodne z § 15 punkt 1 rozporządzenia KRI;

[4] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[5] Sprawozdanie z zadania audytowego podpisane z dniem 30 stycznia 2024 r.
[6] Dalej: wniosek.
[7] Dalej: CPPC lub Grantodawca.
[8] Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego.
[9] Umowa nr FERC.02.02-CS.01-001/23/0408/FERC.02.02-CS.01-001/23/2024. Dalej: umowa o powierzenie grantu lub umowa o dofinansowanie.
[10] Dalej: Projekt.
[11] Z tego z Budżetu Państwa - 135 718,41 zł, budżet środków Unii Europejskiej – 712 521,61 zł.
[12] Według stanu na 20 sierpnia 2025 r.
[13] Dz. U. poz. 773, dalej: rozporządzenie KRI.

– zainstalowania na serwerze przeznaczonym do zapewnienia bezpieczeństwa informatycznego innej aplikacji dziedzinowej, co było niezgodne z § 15 punkt 1 rozporządzenia KRI.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[14] kontrolowanej działalności

OBSZAR

1. Opracowanie i przyjęcie gminnych programów profilaktyki i rozwiązywania problemów alkoholowych oraz przeciwdziałania narkomanii

Opis stanu faktycznego

1. W *Strategii Rozwoju Gminy Wilkowice do roku 2030 pn. „Gmina Wilkowice 2030"*[15] w ramach celu operacyjnego *Odpowiedzialne zarządzania* (4.3.)[16] uwzględniono zagadnienia dotyczące zwiększenia poziomu bezpieczeństwa.

W części dotyczącej *Monitoringu, ewaluacji i aktualizacji dokumentu wskazano, że Analiza powinna uwzględniać wskaźniki określone w ramach planu operacyjnego Strategii, z których kluczowe znaczenie mają wskaźniki zgromadzone (...), którym przypisano trend docelowy. Mogą one być poszerzane lub ewentualnie zamieniane, zgodnie z potrzebami systemu monitorowania i ewaluacji. (...) Analiza wskaźnikowa realizowana jest cyklicznie, najlepiej raz do roku.* W Strategii w zakresie celu operacyjnego Odpowiedzialne zarządzanie wskazano kierunki, oczekiwane rezultaty, wskaźniki oceny osiągnięcia rezultatów, oczekiwane trendy, podmioty odpowiedzialne (Urząd) i zaangażowane i tak, poszczególnym kierunkom działań związanych z cyberbezpieczeństwem przypisano następujące wskaźniki:

- *Wzrost poziomu dostępności do usług publicznych oraz rozwój usług publicznych, w tym usług elektronicznych*, *Zwiększenie dostępności do usług publicznych* (oczekiwane rezultaty), którym przypisano wskaźnik *Liczba oferowanych e-usług;*

- *Podnoszenie kompetencji pracowników samorządowych, Wzrost wykwalifikowania kadry pracowniczej i zarządczej* (oczekiwane rezultaty), którym przypisano wskaźnik *Liczba osobodni szkole;*

- *Monitorowanie jakości usług publicznych, Poznanie ocen i opinii mieszkańców na temat dostępnych, Poznanie ocen i opinii mieszkańców na temat dostępnych usług publicznych, Ewaluacja systemu świadczeń usług publicznych; Poziom zadowolenia mieszkańców z pracy urzędu (oczekiwane rezultaty);* którym przypisano wskaźniki *Poziom zadowolenia mieszkańców z pracy urzędu.*

W zakresie ww. kierunków działań określono oczekiwany trend wzrostowy.

(akta kontroli str. 45-48)

---

[14] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.

[15] Przyjętej uchwałą nr LII/478/2023 Rady Gminy Wilkowice z dnia 1 marca 2023 r. w sprawie przyjęcia Strategii Rozwoju Gminy Wilkowice do roku 2030 pn. „Gmina Wilkowice 2030". Dalej: Strategia.

[16] Ujęty w celu strategicznym (4) pn. *Wzrost jakości życia mieszkańców z jednoczesnym zachowaniem walorów przyrodniczych* w ramach obszaru strategicznego *pn. Zrównoważony i odpowiedzialny rozwój przestrzenny Gminy.*

Wójt w wyjaśnieniach podał, że w zakresie pierwszego kierunku działań w chwili obecnej nie badano tendencji wzrostowej, jak i nie prowadzono badań poziomu zadowolenia mieszkańców z pracy urzędu, natomiast w zakresie podnoszenia kompetencji przeszkolono pracowników. W kolejnych wyjaśnieniach podał, że nie prowadzono badań tendencji wzrostowej, gdyż zapisy w Strategii nie nakładają bezwzględnego obowiązku prowadzenia ich raz w roku.

(akta kontroli str. 36-44, 703-708)

2. W Urzędzie potrzeby w zakresie zwiększenia poziomu cyberbezpieczeństwa ujęto w Strategii oraz audycie wewnętrznym B*ezpieczeństwo informacji w 2023 r.* Przywołano w nim audyt zewnętrzny, którego celem było wykonanie diagnozy cyberbezpieczeństwa w ramach programu *Cyfrowa Gmina*, gdzie m.in. wskazano na brak szczegółowych planów przywracania usług IT, brak dokumentacji ciągłości działania zawierającej szczegółowo określony wykaz podstawowych systemów teleinformatycznych użytkowanych w jednostce z gradacją ich ważności/krytyczności oraz nie określono parametrów RTO[17], RPO[18]. Jednostki organizacyjne Gminy, nie brały udziału w realizacji Projektu, oraz identyfikacji potrzeb w zakresie cyberbezpieczeństwa. W wyjaśnieniach Wójt podał, że Urząd nie posiada zdefiniowanego zakresu działań, który jest kluczowy w zakresie zwiększenia poziomu cyberbezpieczeństwa. Poza audytami nie przeprowadzano analizy uzyskanych efektów. Projekt jest w trakcie realizacji i nie został jeszcze zakończony i rozliczony, a przeprowadzenie analizy efektów będzie zasadne po pełnej realizacji projektu.

(akta kontroli str. 217-230, 633-638, 713-731)

W 2023 r.[19] w Urzędzie Inspektor Danych Osobowych[20] przeprowadził analizę ryzyka w obszarze danych osobowych, arkusze oceny ryzyka danych uwzględniały m.in. zagrożenia i postępowanie z ryzykiem. W zakresie postępowania z ryzykiem w ramach procesu przetwarzania danych osobowych, zostały zidentyfikowane również potrzeby z zakresu cyberbezpieczeństwa m.in. wskazano na:

1 - wdrożenie przygotowanej dokumentacji SZBI, której nie wdrożono z uwagi na zamiar realizacji projektu Cyberbezpieczny Samorząd;

2 - należy zrobić sprawdzenie w zakresie przeglądu dokumentacji/środków bezpieczeństwa konfiguracji-strony/BIP-u/mediów społecznościowych;

3 - w zakresie Prowadzenia Archiwum Zakładowego – należy monitorować ryzyko i w razie pojawienia się rozwiązań technicznych, które mogłyby rozwiązać problem, złożyć rekomendacje.

Ponadto w Urzędzie przeprowadzono: Sprawdzenie zgodności przetwarzania danych osobowych na stanowisku kadr (luty-maj 2023 r.), oraz Sprawdzenie zgodności przetwarzania w zakresie zasady czystego biurka/ekranu (luty-marzec

[17] RTO to maksymalny akceptowalny czas potrzebny na przywrócenie systemów IT i procesów biznesowych po awarii

[18] RPO to maksymalna ilość danych, którą firma jest w stanie stracić, mierzone w czasie od ostatniej prawidłowej kopii zapasowej do momentu wystąpienia awarii.

[19] Wykonaną w okresie od 24 listopada 2023 r. do 5 grudnia 2023 r.

[20] Dalej: IOD.

2024 r.). W Urzędzie ostatnią analizę ryzyka przeprowadzono od 24 listopada 2023 r. do 5 grudnia 2023 r., a po tym okresie Urząd nie przeprowadzał analizy ryzyk z częstotliwością określoną w *Procedurze zarządzania ryzykiem bezpieczeństwa*[21]*, co opisano w Sekcji stwierdzone nieprawidłowości.*

(akta kontroli str. 635-687, 701-731, 1060)

3. Urząd w dniu 21 sierpnia 2024 r. przekazał[22] do NASK wypełnioną *Ankietę dojrzałości do projektu: Cyberbezpieczny Urząd Gminy w Wilkowicach*[23]*,* w terminie 30 dni od dnia zawarcia umowy o powierzenie grantu, zgodnie z § 4 ust. 1 pkt 4a umowy grantowej. W Ankiecie dojrzałości m.in. podano: że 56 pracowników z 73 było użytkownikami systemów IT[24]*.*

(akta kontroli str. 81-90)

W wyniku oględzin[25] ustalono, że ww. ankietę Urząd przesłał przez system obiegu dokumentów FINN (połączony z ePUAP-em) wraz z pismem przewodnim, którego załącznikiem była Ankieta dojrzałości[26].

(akta kontroli str. 999-1004)

4. Urząd przystąpił do Rządowego Programu „Cyberbezpieczny Samorząd". Program został sfinansowany ze środków unijnych, w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC)[27]**.** Umowa o dofinansowanie na realizację Projektu (powierzenie grantu) „Cyberbezpieczny Urząd Gminy w Wilkowicach" została zawarta 26 lipca 2024 r.[28] pomiędzy Skarbem Państwa reprezentowanym przez CPPC (Grantodawcą) a Gminą Wilkowice (Grantobiorcą). Zgodnie z postanowieniami umowy, Gmina jest zobowiązana do zrealizowania Projektu w zakresie rzeczowym w okresie maksymalnie 24 miesięcy od dnia jej wejścia w życie, ale nie dłużej niż do 30 czerwca 2026 r. Wartość dofinansowania (grantu) wynosiła 848 240,02 zł i stanowiła 92 % kosztów kwalifikowanych projektu (w tym dofinansowanie 77,28 % z UE i 14,72 % z budżetu państwa), a kwota wkładu własnego 285 819,98 zł (w tym wkład własny z wydatków kwalifikowalnych 73 759,98 zł). Całkowita wartość projektu wynosiła 1 134 060 zł (w tym wydatki kwalifikowalne 922 000 zł). Okres realizacji projektu od 26 lipca 2024 r. do 30 czerwca 2026 r.[29] Umowa o powierzenie grantu nie była aneksowana. Zakres rzeczowy projektu został wskazany we wniosku i obejmował realizację zadań w trzech obszarach określonych w *Regulaminie Konkursu Grantowego Cyberbezpieczny Samorząd*[30]*,* tj. w obszarze kompetencyjnym, technicznym i organizacyjnym.

(akta kontroli str. 93-143)

---

[21] Wprowadzonej Zarządzeniem nr 52/2018 z dnia 25 maja 2018 r. w sprawie wprowadzenia w Urzędzie Gminy w Wilkowicach dokumentacji dostosowanej do RODO.
[22] Za pośrednictwem systemu FINN 8 SQL.
[23] Dalej: Ankieta dojrzałości.
[24] Wg danych liczba pracowników zatrudnionych po 2 latach od rozliczenia grantu.
[25] Przeprowadzonych w dniu 19 sierpnia 2024 r.
[26] Spakowana do formatu ZIP, plik zawierał ankietę i podpis elektroniczny.
[27] Priorytet II: Zaawansowane usługi cyfrowe. Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny samorząd o numerze FERC.02.02.-CS.01-001/23.
[28] Pod numerem FERC.02.02-CS.01-001/23/0408/FERC.02.02-CS.01-001/23/2024.
[29] Numer wniosku o dofinansowanie (systemowy identyfikator wniosku): f3fe6362-71c2-4f5b-b878-85d5faed5722.
[30] https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad

W obszarze kompetencyjnym wniosek obejmował realizację zadania pn. *Szkolenia z zakresu cyberbezpieczeństwa*, wartość wydatków na zadanie łącznie oszacowano na 129 150 zł, w tym dofinansowanie w wysokości 96 600 zł (co stanowiło 11,4% wnioskowanej kwoty grantu), wkład własny 8 400 zł, oraz wydatki niekwalifikowalne 24 150 zł.

W obszarze technicznym wniosek obejmował *realizację zadania pn. Zakup sprzętu i oprogramowania niezbędnego do podniesienia poziomu cyberbezpieczeństwa, wartość wydatków na zadanie oszacowano na 955 710 zł*, dofinansowanie w wysokości 714 840,02 zł (84,3% wnioskowanej kwoty grantu), wkład własny 62 159,98 zł, oraz wydatki niekwalifikowalne 178 710 zł.

Z kolei w obszarze organizacyjnym wnioskiem objęto zadanie pn. *Aktualizacja SZBI oraz audyt bezpieczeństwa wdrożonego systemu*, które oszacowano na 49 200 zł, dofinansowanie w wysokości 36 800,00 zł (co stanowiło 4,3% wnioskowanej kwoty grantu), wkład własny 3 200,00 zł, oraz wydatki niekwalifikowalne 9 200 zł.

(akta kontroli str. 135-143)

Stosownie do zapisów § 2 ust. 7 pkt 1 umowy grantowej dofinansowanie na realizację projektu miało być wypłacone w trzech transzach tj. 30%, 30% i 40% kwoty wydatków kwalifikowalnych Projektu. Gmina otrzymała środki z CPPC na wyodrębniony rachunek bankowy w dwóch transzach, pierwszą 10 września 2024 r.[31] w kwocie 254 472,01 zł (tj. po przekazaniu ankiety dojrzałości cyberbezpieczeństwa); oraz drugą i trzecią w jednej transzy po złożeniu wniosku o wypłatę całości grantu bez podziału na transze (wniosek z 17 grudnia 2024 r.), która wpłynęła 17 stycznia 2025 r. w wysokości 593 768,01 zł, co było zgodne z postanowieniami § 2 ust. 8 cyt. umowy.

(akta kontroli str. 93-143)

Wójt w wyjaśnieniach podał, że projekt jest w trakcie realizacji, nie złożono wniosku rozliczającego, planowany termin złożenia rozliczenia do końca grudnia 2025 r. Na dzień 20 sierpnia 2025 r. łączna kwota wydatków na realizację projektu wyniosła 1 131 999,75 zł (z czego dofinansowanie ze: środków budżetu państwa 135 471,84 zł, środków UE 711 227,16 zł i środków własnych 285 300,75 zł), a wykorzystano grant w wysokości: 846 699,00 zł[32], natomiast planowany zwrot niewykorzystanych środków wyliczono na kwotę 1 541,02 zł. Naliczone na dzień 30 czerwca 2025 r. odsetki na wyodrębnionym rachunku bankowym naliczone wynosiły 229,59 zł.

(akta kontroli str. 23-26, 36-44, 1026-1045, 1238-1239)

Gmina Wilkowice zawarła ze spółką z o.o. jedną umowę kompleksową na realizację całego zakresu rzeczowego Projektu z dniem 7 listopada 2024 r., firma została wybrana w trybie podstawowym z możliwością prowadzenia negocjacji zgodnie z ustawą z dnia 11 września 2019 r. Prawo zamówień publicznych[33], w kryteriach oceny ofert wyłoniony Wykonawca uzyskał łącznie 100 pkt (tj. cena

[31] Przelew zaksięgowano na rachunku bankowy Gminy w dniu 11 września 2024 r.
[32] Co stanowi 99,8% przyznanego dofinansowania.
[33] T.j. Dz.U. z 2024 r. poz. 1320 ze zm.

60 pkt i 40 pkt termin realizacji przedmiotu zamówienia) czyli o 21 pkt więcej niż drugi oferent. Przedmiotem umowy było *wdrożenie systemu zwiększającego cyberbezpieczeństwo Urzędu Gminy Wilkowice wraz z dostawą niezbędnego sprzętu i oprogramowania*, a zakres przedmiotu opisany w SWZ obejmował w szczególności: dostawę i konfigurację sprzętu; dostawę i konfigurację zaawansowanych systemów bezpieczeństwa; przeprowadzenia szkoleń z zakresu bezpieczeństwa dla wszystkich pracowników; opracowanie i dostosowanie do wdrożonych rozwiązań dokumentów SZBI oraz PBI; przeprowadzenie audytu pograntowego, oraz świadczenie usługi serwisowej, aktualizacji oprogramowania do najnowszych wersji i wsparcia na okres 24 miesięcy.

(akta kontroli str. 146-165, 1064-1229)

W ramach Projektu zrealizowano ww. zadania, nie wystąpiły opóźnienia w realizacji grantu. Umowa i załączniki z CPPC nie przewidywały harmonogramu działań. Gmina zrealizowała zadania zgodnie z harmonogramem rzeczowo-finansowy określonym w umowie z Wykonawcą. Na potrzeby realizacji Projektu wyodrębniono: konto bankowe, oraz analitycznie konta księgowe i sposób finansowania tego Projektu z odpowiednią klasyfikacją budżetową. Łączna wartość zakupionych urządzeń w ramach projektu wynosiła 524 379,75 zł, co stanowiło 61,8% łącznej kwoty grantu określonej w umowie o dofinansowanie.

(akta kontroli str. 23-26, 36-43, 1026-1045)

5. Umowa do dofinansowanie wraz z wnioskiem o przyznanie grantu nie przewidywała udziału jednostek gminnych Urzędu. Wójt w wyjaśnieniach podał, że w ramach przygotowań do złożenia wniosku o dofinansowanie pracownik Urzędu przesłał do ośmiu z trzynastu gminnych jednostek organizacyjnych: wiadomość (e-mail) o możliwości pozyskania środków zewnętrznych w ramach programu Cyberbezpieczny Samorząd i informację z prośbą o złożenie potrzeb w zakresie infrastruktury informatycznej zapewniającej bezpieczeństwo. Z osobami zarządzającymi w pozostałych jednostkach gminnych przeprowadzono rozmowy, dlatego nie zostały one powielone w mailu. Żadna z trzynastu gminnych jednostek organizacyjnych nie zgłosiła zapotrzebowania w przedmiotowym zakresie.

(akta kontroli str. 36-44, 93-122, 703-709, 743)

6. W związku z realizacją Projektu Zarządzeniem nr 193/2024 Wójta Gminy Wilkowice z dnia 1 października 2024 r. został powołany Zespół projektowy celem realizacji (wdrożenia), rozliczenia rzeczowego i finansowego oraz utrzymania efektów projektu. W skład zespołu wchodziło siedem osób, tj.: Wójt, trzech Inspektorów ds. zamówień i funduszy strukturalnych, Informatyk, Inspektor Ochrony Danych Osobowych, oraz Inspektor ds. księgowości budżetowej.

(akta kontroli str. 197-198, 338-344)

7. W okresie objętym kontrolą nie wystąpiła fluktuacja kadr mogąca mieć wpływ na realizację Projektu, jedyna zmiana dotyczyła stanowiska Inspektora ds. zamówień i funduszy strukturalnych, który został przeniesiony na stanowisko

Sekretarza Gminy z dniem 16 kwietnia 2025 r. Wójt w wyjaśnieniach podał, że zmiana ta nie miała wpływu na realizację Projektu.

(akta kontroli str. 309-324)

8. We wniosku o przyznanie grantu[34] Gmina nie określiła wskaźników produktu i rezultatu.

(akta kontroli str. 135-143, 452)

W kwestii braku wskaźników w wyjaśnieniach Wójt podał, że*: We wniosku o dofinansowanie (..) nie określono wprost wskaźników produktu i rezultatu. Wniosek sporządzany został w systemie LSI, który niestety nie przewidywał możliwości wyboru lub wpisania tych wskaźników w dostępnych polach. (..) Gdyby wniosek o dofinansowanie został sporządzony nieprawidłowo, Urząd zostałby wezwany do uzupełnienia brakujących wskaźników. Taka sytuacja nie miała miejsca. Ponadto wniosek został zaakceptowany w systemie, zatwierdzony i ostatecznie podpisano umowę o dofinansowanie.* Wyjaśnił też, że: *(...) Gmina jest obecnie na etapie wdrażania i przygotowywania projektu „Cyberbezpieczny Urząd Gminy w Wilkowicach" do rozliczenia. Wartość wskaźnika rezultatu zgodnie z Załącznikiem nr 9 do Regulaminu Konkursu Grantowego - Opis wskaźników projektu Cyberbezpieczny Samorząd musi zostać osiągnięta w ciągu 12 miesięcy po zakończeniu realizacji projektu, gdzie moment zakończenia projektu został zdefiniowany w umowie o dofinasowanie § 1 pkt 24 jako data zaakceptowania końcowego rozliczenia Projektu przez Operatora*.

(akta kontroli str. 620-625)

Z-ca Wójta[35] w wyjaśnieniach podał, że Gmina 13 sierpnia 2025 r. zwróciła się pisemnie do CPPC w sprawie nieścisłości w zapisach dokumentów dotyczących wskaźników produktu i rezultatu Projektu tj. pomiędzy załącznikiem nr 9 - opis wskaźników Projektu Cyberbezpieczny Samorząd do Regulaminu konkursu Grantowego, a wnioskiem sprawozdawczym (w związku z koniecznością złożenia go do dnia 25 sierpnia 2025 r.). CPPC 14 sierpnia 2025 r. udzieliło następującej odpowiedzi: *Przywoływany przez Państwa załącznik nr 9 zawiera wskaźniki które musi osiągnąć CPPC i NASK-PIB jako Grantodawcy. Państwa obowiązują wskaźniki które ""na sztywno"" są wpisane w formularze wniosków: we wniosek sprawozdawczy i rozliczający zaliczkę.*

(akta kontroli str. 846-853)

W związku z powyższym, w sprawozdaniu z postępu rzeczowego projektu oraz wniosku rozliczającym projekt Wójt podała, że zostaną wykazane następujące wskaźniki rezultatu:

a/ Liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym (kobiety) – szt. zero;

b/ Liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym (mężczyźni) – szt. jedna;

[34] Przesłanego do CPPC 28 listopada 2023 r. i zaakceptowanego 9 stycznia 2024 r.
[35] Z upoważnienia Wójta.

c/ Liczba pracowników podmiotów wykonujących zadania publiczne nie będących pracownikami IT objętych wsparciem szkoleniowym (kobiety) - szt. 37;

d/ Liczba pracowników podmiotów wykonujących zadania publiczne nie będących pracownikami IT objętych wsparciem szkoleniowym (mężczyźni) - szt. 13;

e/ Liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji szt.– sześć;

f/ Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych – szt. 51;

g/ Liczba podmiotów wspartych w zakresie cyberbezpieczeństwa w ramach JST – szt. zero.

(akta kontroli str. 620-625, 846- 853, 1005-1006)

9. W ramach umowy o powierzenie grantu zakupiono następujący sprzęt:

(1)Urządzenia UTM - dwie szt. spełniające funkcję ochrony sieci i bezpiecznego dostępu do Internetu z redundancją ochrony. Urządzenia monitorują komunikację pomiędzy Internetem, a siecią wewnętrzną Urzędu. Dwa urządzenia mają na celu zabezpieczenie przed ewentualną awarią jednego z nich. (2) Deduplikator – jedna szt, urządzenie służące do składowania danych podłączone do serwerów, przechowywujące kopie zapasowe. (3) Tokeny sprzętowe -jeden komplet (20 szt.) służące do zabezpieczenia połączeń zdalnych VPN. (4) Serwer – jedna szt., tj. serwer produkcyjny dla serwerów wirtualnych dostarczonych w ramach Projektu. (5) UPS – pięć sztuk, urządzenia do podtrzymania napięcia urządzeń znajdujących się w serwerowniach. (6) Macierz Dyskowa – jedna sztuka, urządzenie przechowywujące serwery wirtualne dostarczone w ramach Projektu. (6) Oprogramowanie do monitoringu serwerów oraz usług, tj. oprogramowanie do monitorowania infrastruktury IT, które umożliwia zbieranie, analizowanie i wizualizację danych o wydajności, dostępności i stabilności systemów, w tym sieci, stacji roboczych i serwerów. Jest ono używane do śledzenia stanu i integralności różnych komponentów infrastruktury, a także do automatycznego generowania powiadomień o problemach. (7) Oprogramowanie do zarządzania incydentami, które służy do efektywnego zarządzania zgłoszeniami, zbierając je z różnych kanałów komunikacji w jednym miejscu. System zapewnia kontrolę nad zgłoszeniami oraz automatyzację procesów obsługi pracownika. (8) System centralnego zarządzania tożsamością, platforma do zarządzania tożsamością, która pozwala na wdrożenie Single Sign-On (SSO), czyli logowania jednokrotnego, gdzie użytkownik loguje się raz, na podstawie użytkownika i hasła z domeny urzędu. (9) System klasy SIEM z rozszerzeniem EDR, tj. platforma do monitorowania bezpieczeństwa, która integruje funkcje SIEM (Security Information and Event Management) i XDR (Extended Detection and Response). Służy do wykrywania zagrożeń, monitorowania integralności oraz reagowania na incydenty. (10) System dystrybucji alertów bezpieczeństwa, tj. wewnętrzy system Intranetowy informujący użytkowników o zagrożeniach cyberbezpieczeństwa w formie strony internetowej z komunikatami. (11) System zdalnego nauczania, który umożliwia zapoznanie się z materiałami szkoleniowymi.

(12) Oprogramowanie kopii zapasowych, które umożliwia wykonywanie kopii zapasowych serwerów wirtualnych na urządzenia kopii danych.

(akta kontroli str. 166-196, 1055-1057)

W wyniku oględzin[36] ustalono, że wszystkie zakupione przez Gminę urządzenia i oprogramowania zostały zainstalowane, oraz były dostępne z poziomu Administratora. Numery seryjne wszystkich urządzeń były zgodne z protokołami odbiorów. Wszystkie urządzenia znajdowały się w Urzędzie, za wyjątkiem dwóch, które znajdowały się w szkole w tzw. serwerowni zapasowej. Na dzień 10 lipca 2025 r.: system centralnego zarządzania tożsamością był wykorzystywany i przeznaczony wyłącznie dla Administratora; natomiast oprogramowanie do monitoringu usług nie zostało skonfigurowane do stacji użytkowników; oprogramowanie do zarzadzania incydentami nie było udostępnione dla użytkowników; system klasy SIEM z rozszerzeniem EDR nie był podpięty do stacji użytkowników; system dystrybucji alertów bezpieczeństwa, i zdalnego nauczania nie był udostępniony użytkownikom, oraz oprogramowanie kopii zapasowych nie było przez Informatyka wykorzystywane. Informatyk podał, że oprogramowania nie zostały udostępnione i nie są jeszcze w pełni wykorzystywane ze względu na krótki czas od oddania systemów przez Wykonawcę.

(akta kontroli str. 600-612)

Na podstawie kolejnych oględzin NIK przeprowadzonych w Urzędzie w dniu 22 lipca 2025 r., dotyczących maszyn wirtualnych/oprogramowań zainstalowanych na serwerze o nr F6DD334 (zakupionym w ramach umowy o powierzenie grantu), ustalono, że na przedmiotowym serwerze zainstalowano system zdalnego nauczania (bez numeru seryjnego), działanie to było niezgodne z § 15 punkt 1 rozporządzenia KRI, co opisano *w Sekcji stwierdzone nieprawidłowości.*

(akta kontroli str. 616-618)

Na dzień zakończenia czynności kontrolnych NIK Wójt podał, że: (1) Urządzenia UTM - dwie szt. zainstalowano i skonfigurowano 19 grudnia 2024 r. (2) Deduplikator – jedna szt. zainstalowano i skonfigurowano 19 grudnia 2024 r. (3) Tokeny sprzętowe - jeden komplet (20 szt.) na stanie Urzędu (konfiguracja i wydanie użytkownikowi w razie potrzeby do pracy zdalnej). (4) Serwer – jedna szt. zainstalowano i skonfigurowano 20 grudnia 2024 r. (5) UPS - pięć szt. zainstalowano i uruchomiono z dniem 20 grudnia 2024 r. (6) Macierz Dyskowa – jedna szt. zainstalowano i skonfigurowano z dniem 8 stycznia 2025 r. (7) Oprogramowanie do monitoringu serwerów oraz usług zainstalowano 30 stycznia 2025 r. a skonfigurowano dla administratora w dniu 5 marca 2025r. W dniach 18-19 lipca 2025 r. dodano stacje użytkowników do systemu monitorującego. (8) Oprogramowanie do zarządzania incydentami zainstalowano 30 stycznia 2025 r., a skonfigurowano dla administratora w dniu 18 lutego 2025 r. W dniu 19 sierpnia 2025 r. udostępniono system użytkownikom kluczowym w celu przetworzenia zgłoszeń.[37] (9) System centralnego zarządzania

[36] Przeprowadzonych 10 lipca 2025 r. i 14 lipca 2025 r.

[37] Tj. IOD, Sekretarz, Wójt, Wice-Wójt. Oprogramowanie na dzień 20 sierpnia 2025 zostało udostępnione czterem użytkownikom z 51. Administrator posiadał już dostęp. W trakcie

tożsamością zainstalowano 30 stycznia 2025 r., a skonfigurowano dla administratora w dniu 6 marca 2025 r. (10) System klasy SIEM z rozszerzeniem EDR zainstalowano 30 stycznia 2025r. i skonfigurowano dla Administratora w dniu 17 lutego 2025 r. W dniu 18-19 lipca 2025 r. dodano stacje użytkowników do systemu SIEM. (11) System Dystrybucji alertów bezpieczeństwa, zainstalowano 30 stycznia 2025 r., a skonfigurowano dla Administratora w dniu 26 lutego 2025 r. W dniu 18 sierpnia 2025 r. udostępniono ikonkę użytkownikom do zalogowania się do systemu. (12) System zdalnego nauczania zainstalowano 30 stycznia 2025 r. a uruchomiono dla Administratora w dniu 26 lutego 2025 r. Od dnia 19 sierpnia 2025 r. udostępniono samouczek logowania, udostępniono kurs wszystkim pracownikom Urzędu aby mogli zapoznać się z materiałami i wykonać quiz. System wymaga podwójnego logowania hasłem domenowym. (13) Oprogramowanie kopii zapasowych zainstalowano i skonfigurowano dla Administratora w dniu 10 kwietnia 2025 r.

(akta kontroli str. 1055-1057)

Wykonawca na podstawie umowy o powierzenie grantu opracował dwa raporty: (1) Raport ze wstępnego audytu SZBI w Gminie Wilkowice (data utworzenia 27 grudnia 2024 r.), (2) Raport z powdrożeniowego audytu SZBI w Gminie Wilkowice (maj 2025 r.). Wykonawca w trakcie kontroli NIK przekazał Gminie oświadczenie o treści: *Z uwagi na nie przyjęcie w formie zarządzenia nowej Polityki Bezpieczeństwa Informacji w tym Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) przez Gminę Wilkowice, audyt powdrożeniowy został zrealizowany zgodnie z terminem realizacji przedmiotu umowy (określony także w harmonogramie rzeczowo-finansowym) i przedstawia stan na dzień jego przeprowadzenia. Z uwagi na powyższe zobowiązujemy się, że po przyjęciu przez Gminę Wilkowice nowej dokumentacji opracowanej w ramach projektu "Cyberbezpieczny Urząd Gminy w Wilkowicach", przeprowadzimy ponowny, dodatkowy audyt bez żadnych dodatkowych kosztów.*

(akta kontroli str. 1232 –1236)

10. Na dzień zakończenia czynności kontrolnych, nie złożono wniosku rozliczającego grantu. Wójt w wyjaśnieniach podał, że planują złożyć go do końca grudnia 2025 r. Zgodnie z § 3 ust. 1 umowy o powierzenie grantu Gmina zobowiązała się zrealizować Projekt w zakresie rzeczowym wynikającym z Wniosku o przyznanie grantu, w okresie maksymalnie 24 miesięcy od dnia wejścia w życie umowy grantowej, ale nie dłużej niż do 30 czerwca 2026 r. (umowa o powierzenie grantu została podpisana 26 lipca 2024 r.).

(akta kontroli str. 23-26, 36-44, 93-122)

11. W Urzędzie nie został opracowany, ustanowiony i wdrożony kompletny System Zarządzania Bezpieczeństwem Informacji, o którym mowa w § 19 ust. 1

---

planowanego szkolenia prowadzonego przez ASI i IOD użytkownicy zostaną poinformowani które kategorie incydentów należy zgłaszać do systemu oraz zostanie udostępniony system dla użytkowników. Na dzień 20 sierpnia 2025 r. wszyscy pracownicy również mają możliwość zgłaszania incydentów na maila incydent@wilkowice.pl które to zostaną automatycznie zarejestrowane w systemie jako zgłoszenie do opracowania dla Administratora i do wglądu dla użytkowników kluczowych.

w związku z ust. 3 rozporządzenia KRI, co opisano w sekcji *Stwierdzone nieprawidłowości.*

W okresie objętym kontrolą w Urzędzie obowiązywało Zarządzenie nr 52/2018 Wójta Gminy Wilkowice z dnia 25 maja 2018 r. w sprawie wprowadzenia w Urzędzie Gminy w Wilkowicach dokumentacji dostosowanej do RODO, tj. następujących dokumentów: Politykę Bezpieczeństwa Danych Osobowych, Rejestr Czynności Przetwarzania, Instrukcję Zarządzania Systemem Informatycznym, Analizę Ryzyka, Klauzule informacyjne, wzory zgód przetwarzania danych osobowych.

(akta kontroli str. 474-589)

W toku kontroli ustalono, że Procedura zarządzania uprawnieniami ujęta w Instrukcji Zarządzania Systemem Informatycznym wprowadzonej ww. Zarządzeniem określająca zasady przydziału uprawnień do korzystania z zasobów sprzętowych, nie była w Urzędzie stosowna, co opisano *w Sekcji stwierdzone nieprawidłowości.*

(akta kontroli str. 558-589)

12. W Urzędzie w okresie objętym kontrolą, tylko w 2023 r. (tj. od 26 października 2023 r. do 29 grudnia 2023 r.) przeprowadzono audyt wewnętrzny z zakresu *Bezpieczeństwa informacji w 2023 r.,* o którym mowa w § 19 ust. 2 pkt 14 rozporządzenia KRI[38]. W ramach przeprowadzonego audytu sformułowano m.in. następujące zalecenia: *Rozważyć zakup aktualnych pakietów Office; Przeprowadzać dokładną inwentaryzację zainstalowanego oprogramowania.* W zakresie każdego zalecenia wskazano, że osobą odpowiedzialną za ich realizację był Informatyk.

(akta kontroli str. 713-731)

Wójt w wyjaśnieniach podał, że w zakresie zalecenia pn. *Rozważyć zakup aktualnych pakietów Office* zostało ono częściowo zrealizowane, natomiast w zakresie zalecenia dotyczącego przeprowadzenia dokładnej inwentaryzacji zainstalowanego oprogramowania zostało ono zrealizowane.

(akta kontroli str. 312-324, 701-706, 1059)

Urząd na potrzeby kontroli przedłożył tylko audyt wewnętrzny *Bezpieczeństwo informacji w 2023 r. (*od 26 październik 2023 r. - 29 grudnia 2023 r.), po tym audycie w Urzędzie audytor wewnętrzny nie przeprowadzał audytu wymaganego § 19 ust. 2 pkt 14 rozporządzenia KRI, który stanowi, że powinien on być przeprowadzany nie rzadziej niż raz na rok, czyli następny najpóźniej do dnia 28 grudnia 2024 r. co opisano w *Sekcji stwierdzone nieprawidłowości*.

(akta kontroli str. 713-731)

13. Na podstawie § 11 ust. 3 umowy grantowej, w zakresie informacji i promocji Grantobioca zobowiązany był do stosowania zasad określonych w *Podręczniku wnioskodawcy i beneficjenta programów polityki spójności na lata 2021 - 2027*

[38] Audyt: sprawozdanie podpisano 30 stycznia 2024 r.

w zakresie informacji i promocji (opublikowanym na stronie internetowej www.funduszeeuropejskie.gov.pl.). Obowiązek obejmował w szczególności:

1) oznaczenie znakiem Unii Europejskiej, barwy RP, znakiem Funduszy Europejskich, (a) wszystkich prowadzonych działań informacyjnych i promocyjnych dotyczących Projektu; (b) wszystkich dokumentów związanych z realizacją Projektu, podawanych do wiadomości publicznej; (c) wszystkich dokumentów i materiałów dla osób i podmiotów uczestniczących w Projekcie, w tym zaświadczeń o uczestnictwie lub innych certyfikatów, zawierających stwierdzenie, że Projekt jest wspierany przez program operacyjny i finansowany przez UE z danego funduszu;
2) umieszczenie przynajmniej jednego plakatu o minimalnym formacie A3;
3) umieszczenie opisu Projektu na swojej stronie internetowej i w mediach społecznościowych;
4) przekazywanie opinii publicznej i podmiotom uczestniczącym w Projekcie informacji, że Projekt uzyskał unijne dofinansowanie przynajmniej w formie odpowiedniego oznakowania;
5) dokumentowanie działań informacyjnych i promocyjnych prowadzonych w ramach Projektu.

Gmina informowała opinię publiczną o fakcie otrzymania dofinansowania m.in. poprzez: umieszczenie plakatów na trzech tablicach informacyjnych w Urzędzie[39]. Plakaty zawierały wszystkie wymagane oznaczenia, tj. znaki Funduszy Europejskich oraz Unii Europejskiej, nazwę beneficjenta oraz tytuł projektu, a także wysokość dofinansowania i adres portalu mapadotacji.gov.pl. Na stronie internetowej Urzędu oraz w mediach społecznościowych umieszczono informacje dotyczące realizacji Projektu oraz informację o jego dofinansowaniu ze środków Unii Europejskiej. Ponadto dokumenty związane z realizacją Projektu, posiadały wymagane oznaczenia w postaci znaków Funduszy Europejskich, barw RP i Unii Europejskiej. Zrealizowano także obowiązek w zakresie dokumentowania działań informacyjnych i promocyjnych prowadzonych w ramach Projektu, poprzez utworzenie segregatora, w którym przechowywano zrzuty ekranu ze strony internetowej oraz mediów społecznościowych, a także zdjęcia plakatów informujących o projekcie, umieszczonych w Urzędzie.

(akta kontroli str. 23-26, 36-44, 199-216a)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki, w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. W Urzędzie nie został opracowany, ustanowiony i wdrożony kompletny System Zarządzania Bezpieczeństwem Informacji (SZBI), co było niezgodne z § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI. Stosownie do ww. przepisów Urząd Gminy zobowiązany był m.in. do opracowania, ustanowienia, wdrożenia, monitorowania i doskonalenia SZBI, zapewniając poufność, dostępność

[39] Oględziny 30 czerwca 2025 r.

i integralność informacji z uwzględnieniem takich atrybutów jak rozliczalność, autentyczność, niezaprzeczalność i niezawodność.

(akta kontroli str. 474-589)

Wójt wyjaśnił, że *Co prawda, jak wskazano w audycie wstępnym, przeprowadzonym w ramach projektu „Cyberbezpieczny Urząd Gminy w Wilkowicach", obowiązująca w Gminie Wilkowice dokumentacja dotyczy w dużej mierze ochrony danych osobowych. W istotnym zakresie zawiera jednak elementy, które wymagane są na mocy rozporządzenia KRI. (...) Należy także nadmienić, że w 2022 oraz w 2023 r. przeprowadzony został audyt wewnętrzny przez audytora wewnętrznego, w zakresie bezpieczeństw informacji. W audytach tych nie zostały wskazane rekomendacje dotyczące wadliwości obecnie obowiązującej dokumentacji, z tego względu nie podjęto działań w tym zakresie.(...). Podsumowując wyjaśnienia w tym zakresie, stoję na stanowisku, że pomimo niedoskonałości obecnie obowiązującej dokumentacji, zawiera ona elementy Systemu Zarządzania Bezpieczeństwem Informacji, wskazane powyżej.*

(akta kontroli str. 696-698)

Zdaniem NIK, SZBI to kompleksowy zbiór polityk, procedur, procesów i narzędzi, które organizacja stosuje do ochrony swoich zasobów informacyjnych przed zagrożeniami, takimi jak nieautoryzowany dostęp, wycieki danych czy ataki cybernetyczne. Dokumentacja wprowadzona *Zarządzeniem nr 52/2018 Wójta Gminy Wilkowice z dnia 25 maja 2018 r. w sprawie wprowadzenia w Urzędzie Gminy w Wilkowicach dokumentacji dostosowanej do RODO* nie zawierała istotnych dla SZBI procedur, w tym procedury czasu przywrócenia ciągłości działania, procedury typologii sieci, systemowych serwerów wirtualnych; procedury urządzeń brzegowych, jak i Urząd nie miał opracowanych procedur, takich jak: procedura zarządzania konfiguracją; procedura zarządzania zmianami i wykonywaniem testów; polityki fizycznego dostępu do pomieszczeń; procedury zarządzania pojemnością przestrzenią dyskową.

W trakcie kontroli NIK, w Urzędzie ustanowiono SZBI Zarządzeniem nr 125/2025 Wójta Gminy Wilkowice z dnia 8 sierpnia 2025 r. w sprawie przyjęcia PBI oraz Polityki Ochrony Danych Osobowych Gminy Wilkowice (która wchodzi w życie 1 października 2025 r.) w ramach umowy o powierzenie grantu, dlatego NIK odstępuje od sformułowania wniosku w zakresie tej nieprawidłowości.

(akta kontroli str. 744-842)

2. W Urzędzie nie przeprowadzono analizy ryzyka w obszarze przetwarzania i ochrony danych osobowych z częstotliwością określoną w pkt 3.2. obowiązującej Procedury zarządzania ryzykiem bezpieczeństwa wprowadzonej Zarządzeniem nr 52/2018 z dnia 25 maja 2018 r. w sprawie wprowadzenia w Urzędzie Gminy w Wilkowicach dokumentacji dostosowanej do RODO w której przyjęto, że ponowna ocena zidentyfikowanego ryzyka nie może być rzadsza niż co 12 miesięcy, a arkusze ryzyka oceny danych z analizy ryzyka w 2023 r., zostały ostatecznie sporządzone i przekazane do Gminy z dniem 5 grudnia 2023 r., czyli kolejne powinny być ostatecznie opracowane z dniem 6 grudnia 2024 r.

(akta kontroli str. 474-475, 558-589, 1237)

W kwestii braku analiz ryzyka z częstotliwością określoną w cytowanej procedurze Wójt w wyjaśnieniach m.in. podał, że: należy uznać, że przyjęto błędne założenie, iż nie jest konieczne przeprowadzenie ponownej analizy ryzyka, ze względu na realizację projektu (...), a ponowna analiza zostanie przeprowadzona już po jego realizacji z uwzględnieniem wprowadzonych rozwiązań technicznych oraz nowej dokumentacji SZBI.

(akta kontroli str. 1061-1063)

W ocenie NIK, System Zarządzania Bezpieczeństwem Informacji (ustanowienie, wdrożenie i eksploatacja) powinien być oparty na wynikach regularnej analizy ryzyka, gdyż pozwala to na ukierunkowanie działań w zakresie bezpieczeństwa na realne zagrożenia. Analiza ryzyka jest kluczowym elementem wdrażania SZBI, ponieważ pozwala zidentyfikować i ocenić potencjalne zagrożenia, co z kolei umożliwia opracowanie odpowiednich zabezpieczeń i procedur. Obowiązek przestrzegania zarządzenia wewnętrznego oznacza konieczność stosowania się do regulacji w nim zawartych tj. przeprowadzania analiz ryzyka z częstotliwością określoną w procedurze wprowadzonej tym zarządzeniem czyli nie rzadziej niż co 12 miesięcy.

3. Na podstawie oględzin przeprowadzonych w Urzędzie w dniu 22 lipca 2025 r., a dotyczących maszyn wirtualnych/oprogramowań zainstalowanych na serwerze o nr F6DD334 (zakupionym w ramach umowy nr FERC.02.02.-001/23/0408/FERC.02.02.-CS.01-001/23/2024 z dnia 26 lipca 2024 r.) ustalono, że na przedmiotowym serwerze pełniącym funkcje bezpieczeństwa zainstalowano system zdalnego nauczania LearnDash – Learning Management System (LMS) Plugin for WordPress / Liquid Web, Inc. (bez numeru seryjnego). Działanie to było niezgodne z § 15 punkt 1 rozporządzenia Rady Ministrów z 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (dalej: KRI) mówiącym, że *Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk*.

(akta kontroli str. 616 – 619)

W kwestii instalacji na serwerze systemu zdalnego nauczania Wójt wyjaśnił, że wskazane *oprogramowanie LearnDash zostało zainstalowane na przedmiotowym serwerze fizycznym, ale w ramach oddzielnej (dedykowanej) maszyny wirtualnej, odseparowanej logicznie od pozostałych maszyn z usługami tj. system monitoringu czy SIEM. System LearnDash, podobnie jak inne wdrażane systemy bezpieczeństwa przeznaczony był do wewnętrznych zastosowań Urzędu i nie był on nigdy dostępny z sieci internet. (...) Na serwerze uruchomione są wyłącznie maszyny wirtualne utworzone w ramach przedmiotowego projektu, zawierające systemy dostarczone w ramach projektu „Cyberbezpieczny Samorząd*.

(akta kontroli str. 733-734)

Zdaniem NIK, takie rozwiązanie, mimo zastosowania na serwerze hipernadzorcy klasy enterprise (VMware ESXi), narusza zasadę separacji funkcji, zgodnie z którą systemy bezpieczeństwa i aplikacje użytkowe nie powinny współdzielić tego samego serwera.

Współistnienie tych systemów zwiększa ryzyko eskalacji (podniesienia) uprawnień, ponieważ aplikacja webowa – nawet jeśli nie jest dostępna z Internetu – może stanowić wektor ataku w sieci wewnętrznej. Dodatkowo prowadzi to do potencjalnego konfliktu o zasoby serwera, co obniża stabilność i niezawodność systemów bezpieczeństwa.

NIK wskazuje również, że takie wykorzystanie serwera jest niezgodne z celem grantu, którego środki powinny służyć wyłącznie zwiększeniu poziomu bezpieczeństwa. Serwer powinien być zatem wykorzystywany wyłącznie do uruchamiania systemów bezpieczeństwa wdrożonych w ramach projektu, a wszelkie dodatkowe aplikacje powinny działać na odrębnej infrastrukturze.

4. W toku kontroli ustalono, że w Urzędzie nie była stosowana Procedura zarządzania uprawnieniami ujęta w Instrukcji Zarządzania Systemem Informatycznym wprowadzonej Zarządzeniem nr 52/2018 z dnia 25 maja 2018 r. w sprawie wprowadzenia w Urzędzie Gminy w Wilkowicach dokumentacji dostosowanej do RODO w zakresie przydziału uprawnień do korzystania z zasobów sprzętowych.

(akta kontroli str. 1237)

Wójt w wyjaśnieniach z 18 lipca 2025 r. podał, *że nie korzystano z zapisów w Instrukcji (...). Obecnie wykształciła się praktyka niezgodna z Instrukcją, polegająca na ustnym wskazywaniu Administratorowi Systemów Informatycznych zakresu uprawnień koniecznego do nadania użytkownikowi. W opinii kontrolowanego, powyższe spowodowane jest zbyt sformalizowanym wzorem wniosku, określonym w obecnie obowiązującej Instrukcji. W opracowanym w trakcie realizacji projektu „Cyberbezpieczny Urząd Gminy w Wilkowicach, projekcie nowej PBI, proces ten został odformalizowany, co ma na celu umożliwienie sprawnego nadawania uprawnień, bez zbędnych wniosków w formie papierowej, przy jednoczesnym zagwarantowaniu kontroli nad systemem nadawania uprawnień.*

(akta kontroli str. 620-625)

W ocenie NIK, nie stosowanie w Urzędzie przedmiotowej procedury wprowadzonej wewnętrznym Zarządzeniem, to zaniechanie, które rodzi konsekwencje braku pisemnych informacji o przyznanych uprawnieniach do systemów informatycznych oraz uniemożliwia szybkie odtworzenie jakie zasoby posiadał dany użytkownik w przypadku ich utracenia.

5. W Urzędzie po audycie wewnętrznym *Bezpieczeństwo informacji w 2023 r.* przeprowadzonym w okresie od 26 października 2023 r. - 29 grudnia 2023 r. (podpisanym przez audytora 30 stycznia 2024 r.), nie przeprowadzono kolejnego audytu z częstotliwości określoną w § 19 ust. 2 pkt 14 rozporządzenia KRI, czyli, nie rzadziej niż raz na rok, czyli audyt w 2024 r. najpóźniej miał być przeprowadzony do 28 grudnia 2024 r.

(akta kontroli str. 1237)

Wójt w związku z powyższym wyjaśnił, że nie przeprowadzono audytu bezpieczeństwa informacji, ponieważ zakładano, że realizacja audytu wstępnego, przeprowadzonego w ramach projektu Cyberbezpieczny Urząd Gminy w Wilkowicach spełnia wymagania określonego w § 19 ust. 2 pkt 14 rozporządzenia KRI. *Jak i podał, że nie są mu znane żadne inne powody odstąpienia od tego obowiązku.*

(akta kontroli str. 278-291, 696-698)

IV. Wnioski

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujące wnioski:

Wnioski

1. Sporządzenie w oparciu o obowiązujące regulacje wewnętrzne analiz ryzyka z identyfikacją ryzyk w obszarze bezpieczeństwa informacji z częstotliwością określoną w regulacjach wewnętrznych.
2. Przeniesienie aplikacji dziedzinowej na serwer nie związany z bezpieczeństwem informatycznym.
3. Zapewnienie aby uprawnienia w systemach informatycznych były nadawane zgodnie z obowiązującym Zarządzeniem w tym zakresie.
4. Zapewnienie prowadzenia przynajmniej raz w roku okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji zgodnie z § 19 ust. 2 pkt 14 rozporządzenia KRI.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne sporządzono w postaci elektronicznej z użyciem kwalifikowanych podpisów elektronicznych.

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK, kierownikowi jednostki kontrolowanej przysługuje *prawo zgłoszenia* na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do Dyrektora Delegatury NIK w Katowicach. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykonania wniosków

Zgodnie z art. 62 ustawy o NIK, należy poinformować Najwyższą Izbę Kontroli, w terminie 21 od otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Katowice, dnia 10 września 2025 r.

Kontroler
Magdalena Śleziak
Specjalista kontroli państwowej

/podpisano elektronicznie/

Najwyższa Izba Kontroli
Delegatura w Katowicach

p.o. Dyrektor
Marcin Wesoły

/podpisano elektronicznie/

Kontroler

Magdalena Śleziak

Specjalista kontroli państwowej

/podpisano elektronicznie/

Najwyższa Izba Kontroli

Delegatura w Katowicach

p.o. Dyrektor

Marcin Wesoły

/podpisano elektronicznie/